IN THE SPECIFICATION

Please amend the specification as follows:

Paragraph 0011 is amended as follows:

Figure 2B is a block diagram of an authorization certificate 220 to be contrasted with the identity certificate [[204]] 202 shown in Figure 2A. The identity certificate 202 shown in Figure 2A associates an identity 204 with a public key 206, while the authorization certificate 220 shown in Figure 2B associates an authorization 222 with a public key 224. Thus, an authorization certificate 220 issued to a third party does not reveal the identity of the third party. The authorization certificate 220 also contains delegated privileges 226 and a validity interval 228. Delegated privileges 226 may include conditions, limitations, and restrictions on those privileges, including scope, time, and context. The validity interval 228 defines if and when the authorization certificate is valid.

Paragraph 0012 is amended as follows:

Traditional identity certificates [[204]] 202 have significant drawbacks, while authorization certificates 220 are capable of delegating limited privileges to a third party, without revealing the identity 204 of the third party, while still providing confidentiality, authentication, integrity, and non-repudiation. Traditional identity certificates [[204]] 202 are implemented according to the X.509 standard, while authorization certificates 220 are implemented according to the SPKI standard. SPKI certificates can directly encode authorizations, while X.509 certificates merely bind public keys to identities. Software applications must subsequently interpret X.509 identities to make authorization decisions using mechanisms subject to additional security risk, such as compromising a database mapping certificate identities to login account names. SPKI certificates also support constrained delegation of authority.

Paragraph 0015 is amended as follows:

Figure 3 is a block diagram of an authorization certificate chain 300. An authorizer is an entity that makes an authorization decision based on a key used to sign a certificate that is recognized, known, and trusted by the authorizer. Any holder of an SPKI ~~cert6ificate~~ certificate

can act as an authorizer. An authorization certificate chain 300 is a sequence of one or more certificates issued by a holder of authorized keys. The chain conveys the authorization where the root key is trusted by prior knowledge. For example, Major has a root key stored on a secure computer system used in creating certificates. In the Fly-By-Night scenario, Major is the authorizer and signer of an authorizer-to-client certificate 304 and E-Commerce signs the client-to-third-party certificate 306.

Paragraph 0023 is amended as follows:

Figure 6 is a block diagram of an example embodiment of the data signal shown in Figure 5 as a Simple Object Access Protocol (SOAP) request 600 and an example method of using it. The SOAP Request 600 comprises header data 602 that comprises an SPKI certificate 604 and a Retrieval Method including a URI 606. First, the third party 404 signs 608 the SOAP request and sends it to the authorizer 400. The authorizer 400 extracts 610 the SPKI certificate from the SOAP request and performs an HTTP "Get" 612 on the URI. The URI invokes 614 a client web server 616 that performs additional processing 618 and returns 620 a certificate 622 issued by the authorizer to the client ~~622~~.